| NODIS Library | Organization and Administration(1000s) | Search |

NASA Procedural Requirements

NPR 1600.1
Effective Date:
November 03, 2004
Expiration Date:
November 03, 2014

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Security Program Procedural Requirements w/Change 2 (4/01/2009)

Responsible Office: Office of Protective Services

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

Chapter 1: Introduction

1.1 Security Responsibilities

1.1.1. The NASA Administrator is responsible for implementing a comprehensive and effective security program for the protection of people, property, and information associated with the NASA mission. The Administrator shall appoint an Assistant Administrator for Security and Program Protection (AA/OSPP).

1.1.2. Security is the direct, immediate, and inherent responsibility of all NASA personnel, contractors, and others granted access to NASA Centers, facilities, information and technology. General security responsibilities are set forth in this chapter. Specific procedural requirements are cited in each subsequent chapter of this NPR.

1.1.3. The AA/OSPP shall:

1.1.3.1. Oversee Agencywide implementation, integration of, and compliance with the NASA Security Program by providing executive management policy direction and ensuring, through Agencywide advocacy, adequate resources are identified and committed to accomplish the security mission in support of the overall NASA mission, NASA Strategic Plan, and National level security requirements.

1.1.3.2. In collaboration with the Chief Information Officer (CIO), develop and implement Agency Information Technology Security policy via NPD 2810 and NPR 2810, and serve as the Agency Certification and Accreditation (C&A) authority for NASA IT.

1.1.3.3. Serve as the Agency Risk Acceptance Authority (RAA) for all NASA Security Program risk management determinations that require a waiver of Agency security requirements. This does not include IT Security RAA, which falls under the CIO.

1.1.3.4. Develop and implement a program to ensure certification and accreditation of Information Technology (IT) resources identified for processing classified national security information (CNSI) and data.

1.1.3.5. Serve as the focal point for Agency Special Access Program (SAP) and Sensitive Compartmented Information (SCI) security activity.

1.1.3.6. Serve as the Agency point of contact with the intelligence community for intelligence matters and ensure development and issuance of policy and requirements related to NASA's counterintelligence program.

1.1.3.7. Ensure law enforcement and investigative activity performed in conjunction with OSPP security responsibilities at NASA installations is developed and implemented consistent with authorities granted under the Space Act, and in concert with the local Office of Inspector General, local, State, and Federal law enforcement agencies, as appropriate.

1.1.3.8. Appoint a qualified senior security professional as Director, Security Management Division (DSMD).

1.1.3.9. Serve as the Agency Critical Infrastructure Assurance Officer (CIAO) responsible for approving all Center proposals for additions and deletions to the Mission Essential Infrastructure (MEI) Inventory List when such proposals are concurred on by the respective Mission Directorate Associate Administrator.

a. Comply with the requirements of Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection.

b. Effectively collaborate with the CIO to ensure critical cyber assets are identified and included in the Mission Essential Infrastructure (MEI) inventory, as appropriate.

1.1.3.10. Establish and implement organizational standards that ensures NASA security programs are appropriately configured, properly staffed with qualified security professionals, and adequately funded to enable each NASA Center to properly and efficiently manage day-to-day security operations while allowing for transition to increased threat environments and emergency scenarios, including appropriate continuity of operations capabilities.

1.1.3.11. Develop and issue, under separate NPR, asset specific physical security vulnerability risk assessment requirements and physical and procedural security standards to ensure consistency and uniformity in application of security measures appropriate for the vulnerabilities identified.

1.1.3.12. Establish and disseminate staffing, equipment, training, and performance standards for security services contractor organizations to ensure security services obtained are professional, comprehensive, uniform, and consistent with NASA requirements.

1.1.3.13. Develop and disseminate Agency antiterrorism program standards and procedures necessary to ensure appropriate response to threats and acts of terrorism on NASA installations and component facilities.

1.1.3.14. Implement and manage procedures for certifying and obtaining accreditation of IT resources that process CNSI and data.

1.1.3.15. In coordination with the NASA Office of General Counsel, ensure development and dissemination of appropriate policy and procedures regarding use and deployment of covert surveillance equipment (CCTV, etc.).

1.1.3.16. Develop and issue interim policy and procedural requirements as necessary to address specific issues.

1.1.4. The NASA CIO is responsible for the NASA-wide Information Technology Security (ITS) program, and shall:

1.1.4.1. Provide advice and assistance to the Administrator and other Senior Management Officials to ensure that Agency ITS goals, priorities, and requirements are effectively and efficiently addressed to protect the Agency's investment in Information Technology (IT).

1.1.4.2. Develop and implement NASA IT Security policy via the issuance of IT Security Procedural Requirements, architectures, standards, and best practices. This includes common security classification schema, which contribute to open, standard, scaleable, interoperable, yet secure IT environments and assess, with the assistance of the Competency Center for ITS, the state of the Agency's ITS posture, and the effectiveness of its IT Security policies.

1.1.4.3. Except as noted in subsection 1.1.5 below, appoint Agency representatives to Federal groups concerned with ITS.

1.1.4.4. Appoint a Competency Center for IT Security (CCITS) responsible for developing ITS architectures, standards, and best practices for the Agency on behalf of the NASA CIO.

1.1.5. Director, Security Management Division (DSMD) shall:

1.1.5.1. Provide overall focus and direction for the NASA security program.

1.1.5.2. Serve as the Agency oversight official for implementation and management of the Agency Federal Arrest Authority Program and Use of Force policy in compliance with 42 U.S.C. 2456a, and 14 CFR part 1203b--Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel.

1.1.5.3. Develop and implement Agencywide policy and procedural requirements to ensure investigation activity is coordinated and/or referred to the local Office of Inspector General, local, State, and Federal law enforcement agencies, as appropriate.

1.1.5.4. Establish and maintain a Central Adjudication Activity at the Headquarters level charged with adjudicating all Agency requests for security clearances for access to CNSI.

1.1.5.5. Deny or revoke security clearances in accordance with the provisions of EO 12968 in strict accordance with due process.

1.1.5.6. Develop and promulgate, subject to coordination with and concurrence by the Office of the General Counsel (OGC), all NASA security policy and procedures.

1.1.5.7. Through periodic site visits, evaluate compliance with this NPR and overall effectiveness of the NASA security program, including effectiveness of NASA IT Security policy and procedures.

1.1.5.8. Manage the Mission Essential Infrastructure Protection Program (MEIPP).

1.1.5.9. Serve as the Senior Agency Official for implementing procedures for managing and safeguarding CNSI.

1.1.5.10. Ensure that the NASA security program operates in compliance with National security policy, homeland security program directives, and other National level regulations.

1.1.5.11. Coordinate, as appropriate, with the Office of the Chief Medical Officer on all matters related to the Mission Critical Space Systems Personnel Reliability Program screening process requiring evaluations and medical determinations from NASA or outside medical authorities.

1.1.5.12. Ensure appropriate physical security and antiterrorism construction standards are developed and published in cooperation with NASA Facilities Engineering Division personnel.

1.1.5.13. Serve as the focal point for NASA representation on all security and national security policy development forums and committees.

1.1.6. Center Directors shall:

1.1.6.1. Provide current and effective security of personnel, property, facilities, operations, and activities at NASA Centers.

1.1.6.2. Ensure the development and management, through the Center Chief of Security (CCS), of written Center specific security program policy and procedural requirements that implement, to the fullest extent possible, the requirements of this NPR.

1.1.6.3. Appoint, with coordination and concurrence of the AA/OSPP, a qualified and experienced CCS with sufficient authority and resources to accomplish National, Agency, and Center security goals and objectives. Minimum qualifications include:

a. Relevant experience in the law enforcement, military intelligence, or security professions.
b. Leadership and managerial experience at a proven level commensurate with the expectations of the CCS position.
c. Ability to obtain and maintain a Top Secret security clearance.

1.1.6.4. In accordance with this NPR, establish, fund, and maintain a comprehensive security program through the CCS. This includes:

a. Personnel, facilities, and equipment necessary to implement and sustain an effective security program.

b. Appropriate training and professional certification of security personnel, as established by the AA/OSPP.

1.1.6.5. When recommended by the CCS and Center CIAO, propose, as appropriate, Critical Infrastructure (CI) and Key Resource (KR) assets for inclusion in the Mission Essential Infrastructure (MEI) Inventory, to the Mission Directorate Associate Administrator.

1.1.6.6. Act as the Risk Acceptance Authority (RAA) for Center security program risk management determinations that do not require waiver of national security requirements.

1.1.6.7. Grant or suspend eligibility for security clearances up to and including Top Secret, with proper coordination with the NASA Central Adjudication Activity. This authority shall be delegated, in writing, to the CCS.

1.1.6.8. Appoint, in writing, a Certifying Authority (CA) responsible for certifying to the Agency Designated Approval Authority (DAA), Center IT resources identified to process classified information.

1.1.7. The CCS shall:

1.1.7.1. Act as the principal advisor and authority to the Center Director in all matters relating to the NASA security program, as established and defined in NPD 1600.2C.

1.1.7.2. With coordination and concurrence of the AA/OSPP, ensure that the Center Security Office is appropriately staffed with qualified and experienced security personnel.

1.1.7.3. To ensure continuity of operations capability, establish the necessary processes and procedures to cross-train staff into other disciplines of the Center's security program, as practical.

1.1.7.4. Develop, implement, and maintain written Center-specific security program policy and security procedural requirements that implement the requirements of this NPR.

1.1.7.5. Direct, plan, control, and evaluate the overall Center security program, regardless of the specific security discipline and processes involved.

1.1.7.6. Through periodic assessments, determine the adequacy of physical security, loss prevention, and antiterrorism programs and recommend improvements to the Center Director.

1.1.7.7. Using all available sources of intelligence information (i.e., NASA CI Program, Local Law Enforcement, NASA Office of Inspector General (OIG), other Federal agencies), continuously evaluate Center and program-level criticality and vulnerabilities, local threats, and prepare appropriate countermeasures tailored to the resources requiring protection, specifically identifying Center Critical Infrastructure and Key Resources, in coordination with the Center CIO and CIAO, for inclusion in the MEI Protection Program.

1.1.7.8. Establish priorities for the effective deployment of Center security resources and processes during routine and emergency situations.

1.1.7.9. Direct and control Center investigative efforts related to NASA security program operations. Ensure appropriate notifications and referrals to local and supporting Federal law enforcement agencies and the NASA OIG are conducted in accordance with this NPR and established formal agreements. [NOTE: Investigations conducted under NPR 1660, NASA Counterintelligence Program Procedural Requirements, are excluded from the requirements of this NPR.]

1.1.7.10. Exercise Original Classification Authority (OCA).

1.1.7.11. Upon written approval by the AA/OSPP, perform duties as the Center Declassification Authority for all Center declassification and classification downgrading activity, as required. With written approval from the AA/OSPP, the CCS may delegate this authority to qualified subject matter experts cleared to the appropriate level and properly trained in classification management. With written approval from the AA/OSPP, the CCS may delegate this authority to qualified subject matter experts cleared to the appropriate level and properly trained in classification management.

1.1.7.12. Initiate the appropriate personnel security investigation and grant interim security clearances up to and including Top Secret, based on information contained in the investigative request, and grant final clearance upon notification from the NASA CAF that an individual has been adjudicated and determined eligible for the clearance requested or suspend security clearances on behalf of the Center Director and the AA/OSPP.

1.1.7.13. Designate a Center Personnel Security Officer who shall:

a. Properly adjudicate all requests for interim clearances per chapter 2.

b. Properly determine contractor employee security reliability per chapter 4.

c. Successfully complete a minimum of two specified personnel security adjudication courses prior to conducting adjudications and maintain current qualifications.

d. Ensure that designated Senior Adjudicators successfully complete three specified personnel security adjudication courses, one of which must be an advanced adjudicator's course, and maintain current qualifications.

1.1.7.14. Ensure Federal Arrest Authority is properly administered at their respective Center and act as the Center Certifying Official for the authority to carry and use concealed or unconcealed firearms by security forces, both NASA civil service personnel and contractor.

1.1.7.15. Notify the OIG of all suspected criminal activity, when appropriate.

1.1.7.16. Integrate and maintain oversight of all Center security activity, including those of tenant organizations to the extent practical.

1.1.7.17. Ensure appropriate training and professional certifications for security staff and armed security force personnel, commensurate with their assigned tasks, weapons, and equipment, as established by the AA/OSPP.

1.1.7.18. Act as the Center Director's primary staff advisor during any security-related crisis or serious incident and as primary point of contact with all external Law Enforcement agencies.

1.1.7.19. Establish and maintain annual security awareness and training programs for

Center employees.

1.1.7.20. Participate as a principal member of Center teams dealing with resolution of workplace violence and protection issues.

1.1.7.21. Serve as a member of property survey boards.

1.1.7.22. Maintain a Center map of the precise jurisdictional boundaries of Center geographical areas, as determined by the Chief Counsel.

1.1.7.23. Develop and maintain personnel identification programs in accordance with established requirements.

1.1.7.24. Provide operational support to the NASA counterintelligence (CI) program, as appropriate.

1.1.7.25. Participate in all facility design reviews and on Center Master Planning Committees to ensure facility physical security and antiterrorism design criteria are appropriately incorporated into individual facility designs and Center Master Plans.

1.1.7.26. Maintain Center security program statistics and provide quarterly reports to the DSMD under the standards set forth in Appendix L.

1.1.7.27. Establish and maintain all organization informational and operational files pursuant to NPD 1440.6G, NASA Records Management and NPR 1441.1D, NASA Records Retention Schedules.

1.1.7.28. Designate, with coordination and concurrence of the AA/OSPP, a qualified and experienced Center Information Assurance Officer (IAO) who shall:

a. Have relevant experience in IT security and information assurance. Note: Having at least one of the following certifications is highly desired:
(1). Information Systems Audit and Control Association (ISACA) as a Certified Information Security Manager (CISM) or Certified Information Systems Auditor (CISA)
(2). International Information Systems Security Certification Consortium (ISC)2 Certified Information System Security Professional (CISSP)

b. Leadership and communication experience at a proven level commensurate with the expectations of the CIAO position.

c. Ability to obtain and maintain a Top Secret security clearance.

d. Fulfill the specific roles and responsibities for a CIAO described in NPR 2810.1.

e. Support Center Security Offices in certification, auditing, and inspection of unclassified IT systems

f. Support Center Security Offices in investigations of IT security incidents as appropriate. [Note: Center IAOs will not possess federal arrest authority credentials and will not be designated as investigators.]

g. Not have concurrent duties as part of the Center IT security staff.

1.1.8. Program, Line Managers, and Supervisors shall:

1.1.8.1. Support the CCS in the implementation of comprehensive security programs and mission-oriented protective services for the Center, along with individual programs and projects.

1.1.8.2. Effectively manage the level of "cleared" personnel and immediately advise the CCS of any changes in the requirements for access to classified national security information or eligibility for security clearance.

1.1.8.3. Employ CCS recommended security and loss-prevention measures within their programs or organizations.

1.1.8.4. In coordination with the CCS, employ Systems Security Engineering processes at program inception and throughout the individual program life cycle as necessary to ensure appropriate protection and accountability of program resources.

1.1.9. The Center CIO shall:

1.1.9.1. Ensure implementation of IT Security policies and develop and implement local IT Security Procedural Requirements, as deemed appropriate.

1.1.9.2. Coordinate with and support the CCS in the protection of classified and unclassified but sensitive information residing on automated systems.

1.1.9.3. Report IT security incidents to the CCS to ensure appropriate action and necessary referral is effected.

1.1.9.4. Provide technical assistance during investigations as requested by the CCS.

1.1.10. Individual employees shall:

1.1.10.1. Report suspicious activity, criminal activity, violations of national security, and other Center security responsibilities to the Security Office.

1.1.10.2. Be aware of and comply with individual responsibilities and roles in maintaining the Agency and Center security program.

1.1.10.3. Protect Government property, CNSI, and sensitive information in accordance with the requirements of this NPR.

1.1.10.4. Cooperate with Center and Agency Security Officials during inquiries and investigations.

1.1.11. The NASA General Counsel or the Chief Counsel of each Center shall provide legal counsel with regard to implementation of this NPR, as appropriate.

1.2 Best Practices

1.2.1. This NPR seeks to establish uniform security program standards across NASA. One way in which to accomplish "standardization" is to develop, implement, qualify, and share "Best Practices." "Best Practices" serves as a model for other NASA security organizations to learn and, where possible, benefit through adoption for use in improving or enhancing their security program. "Best Practices" occur inside and outside the NASA family, in Government or private industry.

1.2.2. The DSMD and CCS shall develop and share "Best Practices" programs and processes, where appropriate.

1.3 Waivers and Exceptions

1.3.1. Centers may occasionally experience difficulty in meeting specific requirements established in the series of NASA Security Program NPRs. The process for submitting requests for waivers or exceptions to specific elements of the NASA Security Program is as follows:

1.3.1.1. The asset, program, or project manager and CCS shall justify the waiver request through security risk analysis: e.g., cost of implementation; effects of potential loss of capability to the Center; compromise of national security information; injury or loss of life; loss of one-of-a-kind capability; inability of the CCS to perform its missions and goals, etc. (a) Justification must also include an explanation of any compensatory security measures implemented in lieu of specific requirements. (b) The waiver request shall be submitted to the Center Director.

1.3.1.2. The Center Director shall either recommend approval or return the waiver request to the CCS for further study or closure. The Center Director shall forward concurrence to the Center's Mission Directorate Associate Administrator.

1.3.1.3. The Mission Directorate Associate Administrator shall forward waiver requests to the Assistant Administrator for Security and Program Protection (AA/OSPP) at Headquarters or return proposals to the Center Director for further study or closure.

1.3.1.4. The AA/OSPP shall return the waiver request to the appropriate Center Director with an approved waiver, for further study, or denial and closure.

1.4 Violations of Security Requirements

1.4.1. Center Directors, Headquarters Operations Director, the AA/OSPP, the DSMD, or the CCS, shall order the removal or debarment of any person who violates NASA Security requirements or whose continued presence on NASA property constitutes a security or safety risk to persons or property. Any determinations to reconsider granting access subsequent to the removal action must receive the concurrence, in writing, of the AA/OSPP.

1.4.2. Anyone who willfully violates, attempts to violate, or conspires to violate any regulation or order involving the NASA Security program is subject to disciplinary action up to and including termination of employment and/or possible prosecution under 18 U.S.C. 799, that provides for fines or imprisonment for not more than 1 year, or both.

1.5 Terms, Abbreviations, and Acronyms

Terms, Abbreviations, and Acronyms used throughout the family of NASA Security program NPRs are defined in Chapter 10, "Glossary of Terms, Abbreviations, and Acronyms."

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

| NODIS Library | Organization and Administration(1000s) | Search |

DISTRIBUTION:
NODIS